

How to Cite:

Selvam, P. M. P., Sujatha, S. S., & Thanammal, K. K. (2022). Bernstein Vazirani deep neural perceptron based certificateless signcryption for secured data communication in cloud. *International Journal of Health Sciences*, 6(S6), 4169–4190.
<https://doi.org/10.53730/ijhs.v6nS6.10581>

Bernstein Vazirani deep neural perceptron based certificateless signcryption for secured data communication in cloud

P. M. Pazhani Selvam

Reg. No: 18123152161002

Research Scholar, Computer Application, Manonmaniam Sundaranar University, Tirunelveli-627012

Email: pmpselvam69@gmail.com

Dr. S. S. Sujatha

Associate professor, Dept. of M.C.A., S.T. Hindu College, Nagercoil-629001

Email: sujaajay@gmail.com

Dr. K. K. Thanammal

Associate professor, Dept. of M.C.A., S.T. Hindu College, Nagercoil-629001

Email: thanaravindran@gmail.com

Abstract--Present day evolutions in providing genuine security in the Cloud Computing Network have been made Certificateless Signcryption model exceedingly acceptable for several applications. However, security and privacy are the paramount area of interests in safeguarding data or data packet as they are said to be highly sensitive. Moreover, with conventional Certificateless Signcryption process found to be computationally laborious and with the discrete operation minimizing the advantages gained from smaller key size, data security is said to be compromised. To address on this issue, in this work, a novel method called, Bernstein Vazirani Deep Neural Perceptron-based Certificateless Signcryption (BVDNP-CS) for secured data communication in cloud computing network is proposed with multiple layers. The proposed BVDNP-CS method consists of one input layer, three hidden layers and one output layer. The BVDNP-CS method in the first layer obtains the data from personal cloud dataset. In the first hidden layer, with security parameter obtained as input, system parameters and master key are generated by means of Multilinear mapping. In the second hidden layer, three keys, i.e., partial private key, private key and public key are generated by utilizing Bernstein-Vazirani Key Generation, therefore reducing the overhead incurred. Followed by the key generation process, the cloud user sends a request to the cloud server via trusted party for acquiring data packet. Upon successful validation cloud server facilitates user

requested data packet in the form of ciphertext by means of Signcryption function. Next, the authorized cloud users obtain original data and improve secure data access via Unsigncryption. Finally, by means of distinct fine tune adaptable weights using steepest descent function error is reduced that ensures data confidentiality. Experimental works are conducted on the parameters such as execution time, overhead and data confidentiality rate. By evaluating the performance with related methods, results show that the data stored in cloud computing network is secured using BVDNP-CS method and computationally efficient.

Keywords---cloud computing network, multi-linear mapping, bernstein-vazirani, signcryption, unsigncryption, steepest descent

Introduction

Over the recent years, Cloud Computing Network is the prominent conceptualization in the evolution of an on-demand network. This type of network bestows access to a recurrent puddle of configurable resources that can be swiftly furnished and delivered with negligible service provider interaction where Infrastructure, Platform, and Software are said to access as a service. Cloud Computing Network furnishes compensation in terms of low cost and comfort of data, but its distinctive characteristic is its security. Data sharing is an essential performance in cloud storage and in Cloud Computing Network, data sharing has escalated rapidly. Secret maintenance and critical data protection are extremely demanding, specifically when data are stored in memory or transferred via communication networks.

A lightweight, provably secure certificateless model that utilizes Fractional Chaotic Maps (FCM) for Group-oriented Signcryption (CGST) called, CGST-FCM was proposed in [1]. The main characteristic of the CGST-FCM method was any group signcrypter may encrypt the data via the Group Manager (GM) and have to send it to the verifier in a seamless manner. This in turn specifies that the legitimacy of the signcrypter data is said to be only verifiable employing the public conditions of group. However, they were not said to be linked to the conforming signcrypter. But on the other hand, the GM was permitted to divulge the signcrypter identity upon occurrence of legal conflict. Therefore, the CGST-FCM method was said to be safeguarded from indistinguishably chosen ciphertext attack (IND-CCA). Moreover, security was also validated with minimal communication cost. Despite improvement observed both in terms of security and communication cost, the overhead incurred was not focused. To address on this aspect, Bernstein-Vazirani Key Generation function is applied in our work cracking the keys quantumly using only one query for three different keys, therefore minimizing the overhead incurred in signcryption process.

A novel data transmission method called, Homomorphic Block Ring Security System called, HBRSS was proposed in [2] to ensure high-security data transmission and data processing in cloud environments. In HBRSS the entire data splitting principle ensures the splitting of data into blocks, packaged

the block data and finally forming a block ring on the basis of the blockchain. With this blockchain type of structure, not only non-tamperability was ensured but also provided and non-destructibility of data, therefore minimizing the memory utilization. Moreover, an enhanced partial homomorphic encryption algorithm was designed with the objective of improving privacy by means of fuzzy processing, therefore reducing the encryption time. Despite minimizing the encryption time involved, however, the data confidentiality rate was not attended. To improve the data confidentiality in our work, Multi-linear Bernstein–Vazirani Signcryption and Unsigncryption is applied that with the aid of distinct fine tune adaptable weights reduces the error rate and therefore increases the data confidentiality.

In [3], a novel variant of cryptography mechanisms were designed with the objective of increasing the cloud computing security with the aid of two distinct layers. The first layer was designed based on the Shannon's theory of diffusion that in turn with split the actual plaintext and key into equal portions. On the other hand, the second layer was designed on the basis of the Central Dogma of Molecular Biology for cryptographic purpose. With these two distinct functions, execution time used in cloud was reduced. Yet another method to ensure end-to-end security utilizing Hybrid Meerkat Clan Algorithm was designed in [4] that in turn improved the security via crow search algorithm. The main objective of any data storage model on cloud remains in data accessing in an easy manner without compromising its security aspect. However, security consideration till now remains the major feature to ensure safety and effectiveness. In [5], a secured data protection method to provide solution to cloud security and safeguard from fake authorized identity user was proposed. Yet another secure data deletion and verification scheme using merkle hash tree and attribute association tree was proposed in [6] to provide security to the cloud user data.

However, the above said method measures only the time and security aspect. Certain other issues or factors, like execution time, overhead and data confidentiality were not taken into consideration. In fact, execution time, overhead and data confidentiality are prerequisite for data security in cloud computing network. The reason is that cloud data receiver at the receiving end cannot be sure that the data received are same as cloud data that was sent by the sender. There may occur a probability that even an unauthorized user in cloud computing network can even modify the stored data intentionally. Also the time and overhead incurred during secure communication has to be ensured because the delay may cause the compromise in data being sent to the intended recipient also. Hence, the validation has to be ensured at the receiving end in a computationally efficient and timely manner.

In this paper, we solve this problem by proposing a Certificateless Signcryption method with multi-linear and multiple layer principles via Deep Multilayer Perceptrons. With the two functions, first, the execution time and overhead incurred is said to be minimized and with the Deep Multilayer Perceptrons principles, it remains laborious and cumbersome process in modifying the data by unauthorized cloud users. On contrary to the traditional method of public and private key system, our method not only permits authorized user to decrypt ciphertext but also permits to validate the source via Bernstein–Vazirani function.

Finally, the security of data in cloud computing network is ensured by applying Certificateless Signcryption/Unsigncryption.

Contributing remarks

In summary, the contributions of the paper include the following:

- We develop a novel Multi-linear Setup Mapping model that is not only computationally efficient in deciphering the data and complicated statistical functions involved makes only authorized user in data extraction, therefore ensuring data security.
- We use the proposed Bernstein–Vazirani Key Generation model to generate a novel partial private key, private key and public key generation that ensures only authenticated and authorized data sharing via trusted party and cloud service provider. The model exhibits several desirable features that include randomly selected filters providing data security via partial, private and public key generated via third party.
- Finally, a detailed security and performance analysis of the proposed method is designed. The computationally efficiency analysis shows that the proposed Bernstein–Vazirani Multi Layer Deep Neural Perceptron-based Certificateless Signcryption for Secured Data Communication in Cloud Computing Network ensures data security in cloud computing network. We compare the performance of the proposed method with other state-of-the-art certificateless signcryption methods in the literature and infer that the proposed method attains comparatively better performance while being provably secure.

Organization of the paper

The remainder of this paper is organized as follows. Section 2 discusses some preliminaries of the paper related to the certificateless signcryption scheme applied in cloud computing network for secured data communication. Section 3 introduces the dataset description, the system model and presents the proposed method Bernstein–Vazirani Multi Layer Deep Neural Perceptron-based Certificateless Signcryption for Secured Data Communication in Cloud Computing Network. Section 4 presents the experimental setup and Section 5 presents the performance evaluation containing execution time, overhead and data confidentiality. Finally, the concluding remarks are provided in Section 6.

Related Works

Cloud computing has manifested to be significant in all fields of applications with the assistance of the cloud network. In this concept, outsourcing to cloud for data storage purposes has become the need of the hour. It is apparent that data storage is the appropriate service in cloud computing network. However, its extensive application is hampered by the unease of experiencing a secure access to data without a contravention on confidentiality and authentication. In [7] queuing theory and novel dynamic process scheduling method on the basis of the queuing theory, for business processes was proposed. With this scheduling method, the issue concerning optimal cloud resource allocation on the basis of

number of tasks and execution stages to enhance security issue for business process was also presented. With the main consideration being information security and privacy method to safeguard information transmission between users from modifying significant data was designed in [8]. With this design multilevel security was ensured for securing data transmission in cloud environments. Yet another lightweight privacy preservation for heterogeneous network was presented in [9]. However, authentication mechanisms were not provided. In [10] a study involving authentication mechanisms for cloud computing network was investigated.

On detail, third-party auditor (TPA) is utilized in cloud computing network to ensure security services. With the immense magnification of demand for services concerning cloud network, regulatory demands, there arise a requirement for a semi to fully automated self sovereign identity (SSI) implementation to minimize cost. A cryptographic method for data migration in a secured manner to and from the cloud network utilizing self sovereignty identity was implemented in [11]. With the involvement SSI peer-to-peer transactions, presence of TPA was no longer required, therefore reducing the cost. However, methods for securely migrating data between cloud and deleting the data permanently from original cloud was not focused. To solve this issue, a novel counting Bloom filter-based method was proposed in [12].

In present day decagons, vast number of protocols for ensuring data integrity in a remote manner has been proposed. In [13], a novel model of RDIC with un-trusted PKG and malicious by utilizing partial key generation and Authentication, authorization, accounting (AAA) service was proposed. Yet another fine grained revocation method via multi authority key generation center to improve storage cost and communication cost was designed in [14]. A survey of data security and privacy protection mechanisms for cloud storage was investigated in [15]. A secure vehicular network model on the basis of IoT and cloud was proposed in [16]. As far as cryptography is concerned, certificateless signcryption (CLSC) is considered as one of the present-day public key techniques that connects the essentials of confidentiality and sensitive data authenticity between users with minimal overhead. In [17], a new data sharing method to ensure safety of data by means of CLSC scheme was proposed. Also, by employing Diffie-Hellman inversion (DHI) both authenticity and confidentiality was assured with minimal overhead. Yet another paper in [18] was proposed to attain both reliability and security in cloud computing environments was proposed via two phase resource sharing method. A survey of privacy preservation mechanisms for secure data storage in cloud network was proposed in [19].

Considering the security requirements of remote healthcare, a robust and lightweight secure access method for cloud-based E-healthcare services was presented in [20]. The proposed method addressed the prospective menaces by ensuring secure interface to users and prohibiting restraining users from information access stored in cloud. With the assistance of multiple keys generated via key derivation function (KDF) end-to-end ciphering of information for mitigating misuse was also provided. Motivated by the above materials and methods, in this work, a novel secure data communication method in cloud computing network utilizing Bernstein-Vazirani Multi Layer Deep Neural

Perceptron-based Certificateless Signcryption is proposed. The elaborate description is provided in the following sections.

Bernstein–Vazirani Multi Layer Deep Neural Perceptron-based Certificateless Signcryption for Secured Data Communication in Cloud Computing Network

The recent evolution of the cloud computing network enables a lot of people to share their data or data packets with other cloud users. The cloud computing network is utilized in permitting data sharing and numerous services to the cloud user and the organization. To ensure efficient data sharing in cloud computing network, only authorized cloud users must be able to get access data packet from the cloud. On the basis of this motivation, in this work, a novel method called, Bernstein Vazirani Deep Neural Perceptron-based Certificateless Signcryption (BVDNP-CS) for secured data communication in cloud computing network. In BVDNP-CS method the new security mechanism is applied to cloud computing network for data sharing and secured access. Figure 1 shows the structure of BVDNP-CS method.

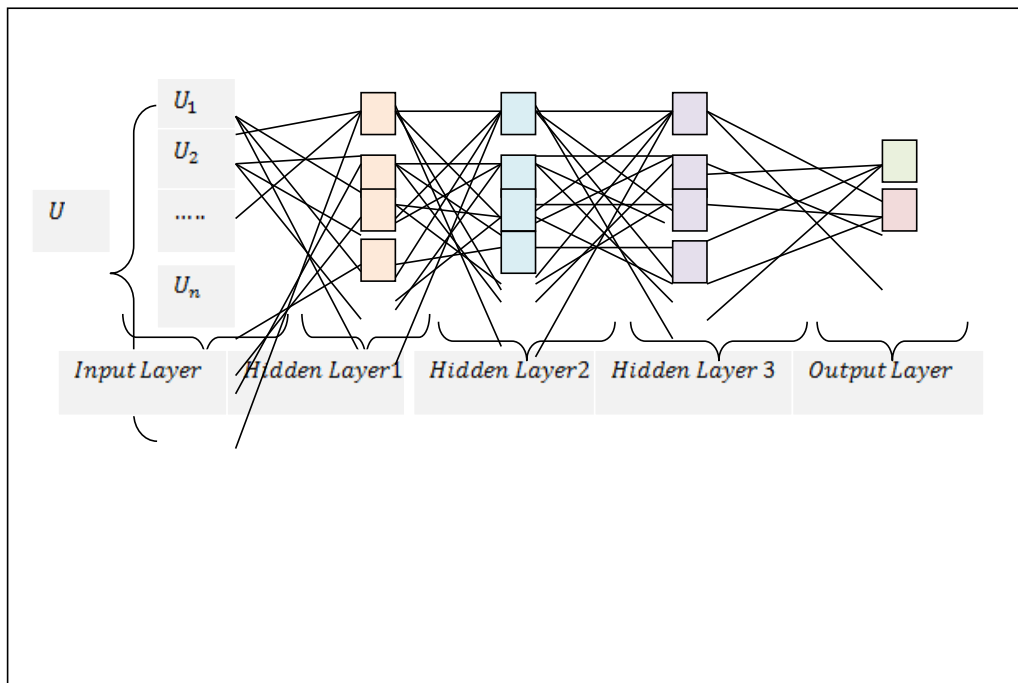


Figure 1. Structure of Bernstein Vazirani Deep Neural Perceptron-based Certificateless Signcryption (BVDNP-CS) method

As shown in the above figure, the Multi Layer Deep Neural Perceptron structure comprises of neurons like nodes are linked from one layer to other consecutive layer. The Multi Layer Deep Neural Perceptron comprises of five layers i.e., an input layer, an output layer and three hidden layers of nonlinearly-activating nodes. As Multi Layer Deep Neural Perceptron is extensively connected, each node (i.e., cloud user) in one layer connects with a certain weight W_i to every node in

the succeeding layer. The features or the column fields obtained from the personal cloud dataset (as in table 1) forms as input nodes to the input layer. In our work, there forms 17 input nodes provided as input to the input layer for secure data communication in cloud computing network. With the input nodes provided as input to the first hidden layer, here setup for secure data communication between cloud users via trusted third party and cloud service provider are said to be established via multi-linear mapping. Forward propagation is employed in the proposed method where inputs from one layer are connected to others with distinct fine tune adaptable or versatile weights forming an entire deep neural network. The input layer has a number of cloud users ' $U = \{U_1, U_2, \dots, U_n\}$ ' and the neuron activities in the input layer ' $x(T)$ ' at time instance ' T ' is mathematically stated as given below.

$$x(T) = \sum_{i=1}^n U_i * W_i + B \quad (1)$$

From the above equation (1), the input layer is modeled based on the cloud user ' U_i ' waiting for data packet ' DP ' transmission at time ' T ' in a secured manner via fine tune adaptable weights ' W_{ij} ' and bias ' B ' respectively in cloud computing network. In the second hidden layer, three types of keys, i.e., partial private key, private key and public keys are generated for each cloud user by the trusted party by employing Bernstein-Vazirani function. Next, in the third hidden layer, signcryption or unsigncryption function is performed by the trusted party via cloud service provider to ensure secure data access in cloud computing network. Finally, the output layer authorized cloud user is permitted to access the data packet whereas the unauthorized cloud users on the other hand are denied with the access. Learning takes place occurs in the perceptron by updating the weights after each piece of data packet is processed (i.e., shared between the authorized cloud user), on the basis of error obtained in the output compared to the expected result.

$$Err_i(n) = TV_i(n) - PV_i(n) \quad (2)$$

From the above equation (2), the error rate in the output node ' i ' in the ' n th' data point is measured based on the targeted value ' $TV_i(n)$ ' and the output value produced by the perceptron ' $PV_i(n)$ ' respectively. The output node weights are fine tuned according to steepest descent function as given below.

$$\Delta W_{ij}(n) = -\eta \frac{\delta Err(n)}{\delta U_j(n)} y_i(n) \quad (3)$$

From the above equation (3), ' $y_i(n)$ ' forms the output of the preceding neuron with ' η ' denoting the learning rate for the corresponding cloud user ' $U_j(n)$ '. In the

sections given below, initially the dataset description is provided, followed by system model and the elaborate description of the BVDNP-CSmethod.

Dataset description

Table 1
Details of personal cloud dataset

S. No	Features	Description
1	Row_id	Database row identifier
2	Account_id	Personal cloud account used perform API call
3	File_size	Size of uploaded/downloaded file
4	Operation_time_start	Starting time of API call
5	Operation_time_end	Finishing time of API call
6	Time_zone	Time zone of node
7	Operation_id	Hash to identify API call
8	Operation_type	PUT/GET API call
9	Bandwidth_trace	Time series trace of a file transfer
10	Node_ip	Network address of node executing this operation
11	Node_name	Host name of node executing this operation
12	Quota_start	Amount of data starting of API call
13	Quota_end	Amount of data ending of API call
14	Quota_total	Overall storage capacity
15	Capped	Indicates if the current node is being capped
16	Failed	Indicates if the API call failed
17	Failure	Includes available failure information of API call

In the proposed method, personal cloud dataset is utilized from the NEC personal cloud trace. The trace file contains 17 features and these seventeen features '**F**' are included in the form of data packets '**DP**' for each user '**U**'. The objective of the proposed method remains in sharing the information from these data packets '**DP**' in a secure manner between users in cloud computing network. Table 1 given below lists the features and their description from the personal cloud dataset.

System model

The system model of the proposed x method cloud network is shown in Figure 2. The proposed method cloud network system model comprises of four entities. They are Cloud Service Provider '**CSP**', Trusted Authority '**TA**', Data Owner '**DO**' and finally the Data User or cloud user or User '**U**' respectively.

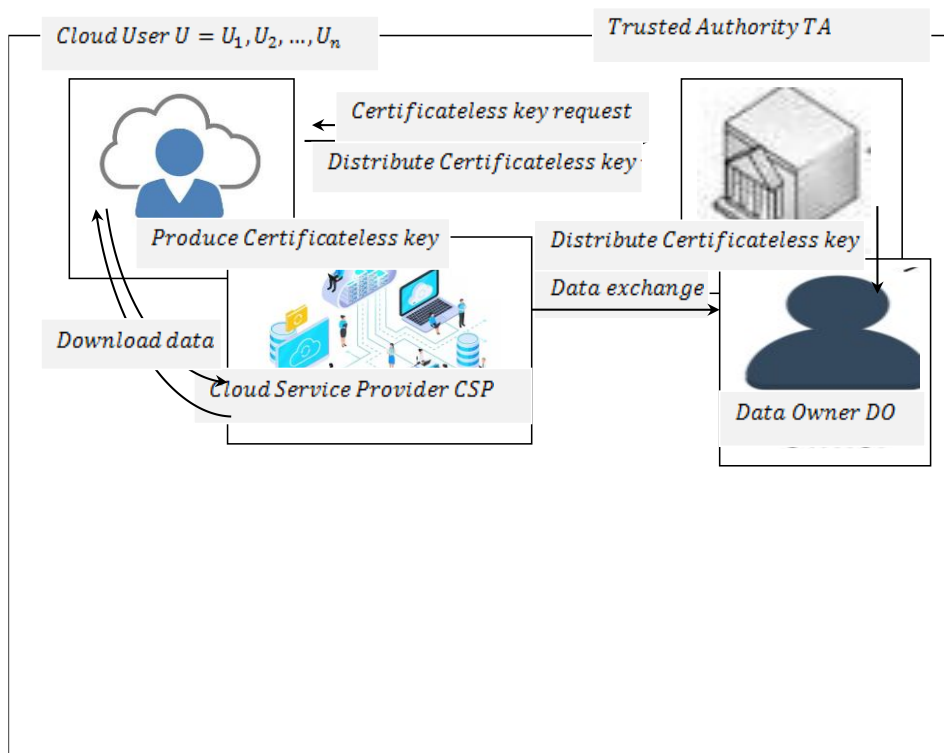


Figure 2. System model of the proposed method

As shown in the above figure, the Cloud service provider '*CSP*' possesses significant computing potentiality, storage resources and imparts several services like, storage of data and distribution of the same for cloud users or users. The second entity is the data user or cloud user or simply user '*U*' requests private key from the '*TA*' via the owned attribute set, and then user '*U*' retrieves data or data packets from the '*CSP*'. The third entity remains the Trusted Authority '*TA*', that establishes the system beginning or initialing procedure, produces master key and public parameter, that in turn safeguards the users' keys in a secured manner.

The Trusted Authority '*TA*' is in charge of registration of the user '*U*' and management of system parameters '*params*'. Finally, the fourth entity is the Data owner '*DO*' that remains the pivotal factor of use in cloud computing network owing to the reason that with the utilization of numerous cloud applications in daily chores results in the increase in data exponentially. Also, with constrained in storage, the '*DO*' leases CSP resources and computing resources for storing and distributing data. Upon successful expiry of the utilized data, the plaintext, ciphertext, and key are said to be deleted in a timely fashion.

Multi-linear Mapping

The certificateless signcryption for secure data transmission in Cloud Computing Network is constructed on Multi-linear Groups. The Multi-linear mapping involves a function that fuses components of several variables that is linear in each of its arguments. The objective behind the utilization of multi-linear mapping in the setup phase is due to the minimum CPU utilization occupied and also cumbersome statistical function involved making extraction insignificant and acquired only by highly securitized format. In the setup phase, to start with a security parameter ' η ' is taken as input. The Trusted Authority ' TA ' executes the Multi-linear Setup Mapping algorithm, to generate system parameters ' $params$ ' a master key ' mk '. Let us consider a security parameter ' η ', then, the multi-linear map is a function stated as given below.

$$f: U_1 * U_2 * \dots * U_n \rightarrow W \quad (1)$$

From the above equation (1), ' $U_1 * U_2 * \dots * U_n$ ' (i.e., cloud user vector space) and ' W ' (i.e., trace vector space) forms the vector spaces, where ' $U_1 * U_2 * \dots * U_n$ ' has dimension ' D_i ' and ' W ' possess dimension ' D ' respectively. With the above said multi-linear mapping, the Trusted Authority ' TA ' obtains the system parameter as given below.

$$params = (\eta, f, D_i, D, DP) \quad (2)$$

From the above equation (1), Trusted Authority ' TA ' publishes the system parameters ' $params$ ' like, the security parameter ' η ', multi-linear map function ' f ', dimension of users ' D_i ', dimensions of traces ' D ' and data packets ' DP ' (possessing 17 features as in table 1) and securely keeps the master key ' mk '. The pseudo code representation of Multi-linear Setup Mapping is given below.

Input: Dataset ' DS ', Features ' $F = F_1, F_2, \dots, F_n$ '
Output: system parameters ' $params$ ', master key ' mk '
1: Initialize ' $n = 17$ ', dimension ' $D_i = 500$ ', ' $D = n = 17$ ', Data packets ' DP ' 2: Begin //Setup 3: For each Dataset ' DS ', Features ' F ' and Users ' U ' 4: Formulate multi-linear map function as in equation (1) 5: Trusted Authority ' TA ' publishes the system parameters ' $params$ ' as in equation (2)

6: Returnsystem parameters '*params*' and master key '*mk*'

7: End for

8: End

Algorithm 1 Multi-linear Setup Mapping

As given in the above Multi-linear Setup Mapping algorithm with the objective of minimizing the CPU utilization, with personal cloud dataset provided as input, for each cloud user, the master key and the corresponding system parameters are generated by utilizing the multi-linear mapping. Here, the multi-linear mapping with sophisticated statistical function obtains the parameters via vector space dimension mapping, therefore reducing the communication cost involved in data communication between users in cloud computing network.

Bernstein-Vazirani Key Generation model

With the data or data packets to be stored in the cloud environment for future communications between users, based on multi-linear mapping setup, in this section, key generation based on Bernstein-Vazirani function is designed. The Bernstein-Vazirani function involves the process of extracting the key (i.e. partial private key/private key/public key) with the objective of securely sharing data or data packets in cloud computing network.

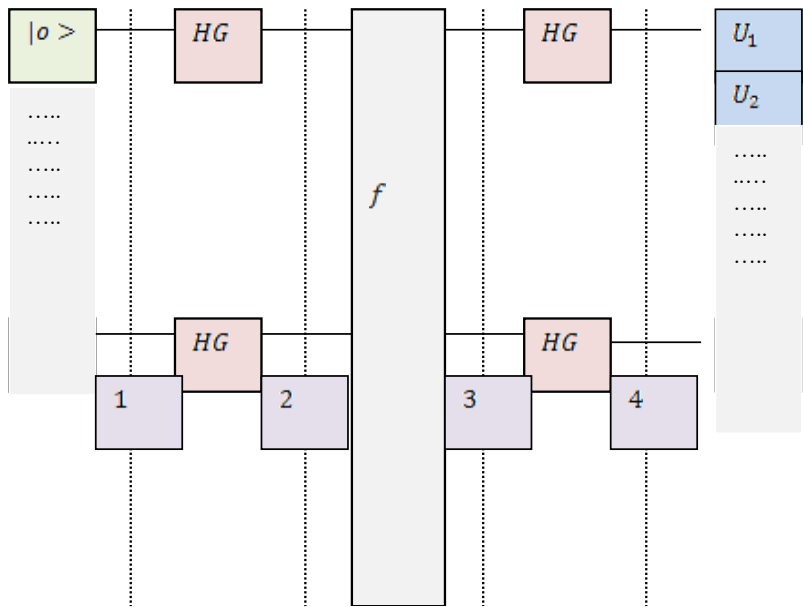


Figure 3. Structure of Bernstein-Vazirani Key Generation model

The Bernstein-Vazirani function encrypts the '0's' and '1's' of a digital signal (i.e. data or data packets) where instead of differentiating between two different

classes of functions (i.e., between the sender user and the receiver user), it tries to obtain a string encoded in a function. Each string encoded in a function represents one piece of information, '0' or '1' for binary code. This code in turn utilizes strings of '0's' and '1's' to produce a logical message. Figure 3 shows the block diagram of Bernstein–Vazirani Key Generation model.

As shown in the above figure, the register for the qubits are set to '0', followed by which the Hadamard Gates '*HG*' are applied for each cloud user, for when the qubit is '*s*' of user ' $U_i = 1$ ', its state is converted to '1' and for when the qubit is '*s*' of user ' $U_i = 0$ ' its state is converted to '0'. The sender now sends the secret string '*s*' via randomly selected filters and records the functions of each dot product between sender user ' U_i ' and secret string ' $s \in \{0,1\}$ '. Now, the sender knows what functions of each dot product the receiver has to be received. Even, if the unauthorized cloud user detects the functions, the information present in the filters is quickly transformed, describing that an unauthorized user is trying to extract the data packet present in the cloud computing network, unauthorized user here cannot obtain the data packets and hence is said to be secured. The partial private key is first identified by evaluating the function '*n*' times with the cloud user ip address (node_ip) and is mathematically stated as given below.

$$f(1000 \dots 0_n = s_1) \rightarrow PPK(U_1)$$

(3)

$$f(0100 \dots 0_n = s_2) \rightarrow PPK(U_2)$$

(4)

...

(5)

$$f(0010 \dots 0_n = s_n) \rightarrow PPK(U_n)$$

(6)

$$PPK(U_i) \rightarrow (params, mk, s_i)$$

(7)

From the above equations (3), (4), (5), (6) and (7), with the obtained partial private key ' $PPK(U_i)$ ', the private key for ' $n: |0\rangle^n$ ' qubit state is mathematically represented as given below.

$$t_i = \frac{1}{\sqrt{2}^n} \sum_{x=1}^n |x\rangle$$

(8)

$$PK(U_i) \rightarrow (params, mk, s_i, t_i)$$

(9)

From the above equations (8) and (9), with the above private key ' PK ' for each cloud user ' U_i ', the public key is obtained as given below.

$$PubK(U_i) \rightarrow (params, s_i, t_i) \quad (10)$$

The pseudo code representation of Bernstein–Vazirani Public and Private Key Generation is given below.

Input: Dataset ' DS ', Features ' $F = F_1, F_2, \dots, F_n$ '
Output: Overhead-minimized Key Generation
1: Initialize data packets ' DP ', system parameters ' $params$ ' and master key ' mk ' 2: Begin 3: For each Dataset ' DS ' with Features ' F ', Data packets ' DP ', system parameters ' $params$ ' and master key ' mk ' and Users ' U ' 4: Generate partial private key as in equation (7) 5: Return partial private key ' $PPK(U_i)$ ' 6: Generate private key as in equations (8) and (9) 7: Return private key ' $PK(U_i)$ ' 8: Generate public key as in equation (10) 9: Return public key ' $PubK(U_i)$ ' 10: End for 11: End

Algorithm 2 Bernstein–Vazirani Key Generation

As given in the above Bernstein–Vazirani Key Generation algorithm, with the objective of enhancing the data security in cloud computing network, three unique keys, i.e., partial private key, private key and public key are generated by employing the Bernstein–Vazirani function. The advantage of Bernstein–Vazirani function remains in solving the problem quantumly or cracking the keys quantumly using only one query contrary to the conventional methods that would take ' n ' queries. This in turn would not only minimize the overhead incurred in key generation but also secure the cloud users data or data packets without modification, hence said to ensure data security significantly. With the three keys generated above, i.e., partial private key, private key and public key, the process of data security in cloud computing network is said to be progressed by scheming signcrypt and unsigncrypt that is described in the forthcoming section.

Multi-linear Bernstein–Vazirani Signcrypt and Unsigncrypt

Given the common parameters ' $params$ ', the data packets ' DP ', and the public key ' $PubK(U_i)$ ', the private key ' $PK(U_i)$ ', the cloud user with identity ' $row_id(U_i)$ ', the cloud service provider ' CSP ' generate the cipher text ' CT ' as the output. This is mathematically expressed as given below.

$$CT \rightarrow SIGNCRYPT(params, DP, PK(U_i), row_id(U_i), PK(U_i)) \quad (11)$$

Given the ciphertext ' CT ', on the other hand, the sender's identity ' $row_id(U_i)$ ', and the public key ' $PubK(U_i)$ ', the receiver with identity ' $row_id(U_j)$ ' and the private key ' $PK(U_j)$ ', the cloud service provider runs this algorithm to unencrypt the ciphertext. This is mathematically expressed as given below

$$DP \rightarrow UNSIGNCRYPT \left(params, CT, row_id(U_i), row_id(U_j), PBK(U_i), PK(U_j) \right) \quad (12)$$

The pseudo code representation of Multi-linear Bernstein–Vazirani Signcryption and Unsigncryption is given below.

Input: Dataset ' DS ', Features ' $F = F_1, F_2, \dots, F_n$ '
Output: Secure data communication
1: InitializeData packets ' DP ', system parameters ' $params$ ' and master key ' mk ', private key ' $PK(U_i)$ ' and public key ' $PubK(U_i)$ ' 2: Begin 3: For each Dataset ' DS ' with Features ' F ' Data packets ' DP ', system parameters ' $params$ ', sender user identity ' $row_id(U_i)$ ' 4: If (target value matches with value produced by perceptron) 5: Then cloud user is said to be authorized 6: Cloud service provider permits access 7: Perform signcryption function as in equation (11) 8: Send digital signature to authorized user 9: End if 10: If (target value does not matches with value produced by perceptron) 11: Then cloud user is said to be unauthorized 12: Cloud service provider does not permits access 13: End if 14: End for 15: For each Dataset ' DS ' with Features ' F ' Data packets ' DP ', system parameters ' $params$ ', receiver user identity ' $row_id(U_j)$ ' 16: Ifdigital signature is valid 17: Perform unsigncryption function as in equation (12) 18: Obtain original data packet ' DP ' 19: End if 20: End for 21: End

Algorithm 3 Multi-linear Bernstein–Vazirani Signcryption and Unsigncryption

As given in the above algorithm, the cloud user who wants to access the data packets initially logs into the cloud computing network with the corresponding database row identifier. If the entered cloud userrow identifiermatches with the cloud server database then the entered cloud user is authorized and hence granted with access and hence referred to as authorized user. As a result, the

cloud service provider permits access to authorized cloud user and performs encryption and signature generation. On the other hand at the cloud user side, the signature is first validated using the public key with which the original data packet is obtained with the private key. Owing to this, secure data access in the cloud computing network is ensured with good data confidentiality.

Experimental setup

Experimental evaluation of the proposed Bernstein Vazirani Deep Neural Perceptron-based Certificateless Signcryption (BVDNP-CS) method is carried out using java language with a CloudSim network simulator. The CloudSim network simulation is a simulation and modeling tool performing \cloud computing services. The entire framework is performed on a distributed server with numerous Virtual Machines connected to it. The dataset is taken from Personal Cloud Datasets: NEC Personal Cloud Trace (<http://cloudspaces.eu/results/datasets>). Experimental evaluation of proposed DMPPALCS technique and two existing algorithms namely Fractional Chaotic Maps (FCM) for Group-oriented Signcryption (CGST) CGST-FCM [1], Homomorphic Block Ring Security System – HBRSS [2] are simulated using the different metrics such as execution time, overhead and data confidentiality.

Discussion

In this section, the efficiency of proposed BVDNP-CS method is analyzed with the above-said metrics using the table and graphical representation. The comparison is made with the BVDNP-CS method and existing methods namely, CGST-FCM [1] and HBRSS [2].

Performance evaluation of execution time

The execution time is defined as the amount of time consumed by the Multi-linear Bernstein–Vazirani Signcryption and Unsigncryption algorithm to perform secure data (i.e., data packet) sharing between cloud users in cloud computing network. The mathematical formulation for execution time is given below.

$$ET = \sum_{i=1}^n DP_i * Time [sharing DP] \quad (13)$$

From the above equation (13), the execution time ' ET ' is measured based on the data or data packets ready for sharing between cloud users ' DP_i ' and the time consumed in sharing data packets ' $Time [sharing DP]$ '. It is measured in terms of milliseconds (ms). Table 2 describes the experimental results of execution time versus the number of cloud user data in the ranges from 25 to 250. Execution time here refers to the amount of time consumption of the BVDNP-CS method in performing a specific task (i.e., data sharing between cloud users in cloud computing network).

Therefore, the execution time involved is also said to be increased while increasing the number of cloud user data. This is proved by means of sample calculation, with '25' data being considered for estimating the execution time for evaluation. The execution time was found to be '3.75 ms' using the BVDNP-CS '5.5 ms' using CGST-FCM [1] and '7.5 ms' using HBRSS [2] respectively. The execution time involved in ensuring secure data communication between cloud users was found to be lesser using BVDNP-CS method when compared to [1] and [2].

Table 2
Tabulation for execution time using BVDNP-CS, CGST-FCM [1] and HBRSS [2]

Number of cloud user data	Execution time (ms)		
	BVDNP-CS	CGST-FCM	HBRSS
25	3.75	5.5	7.5
50	4.15	6.25	9.15
75	5.35	7.45	10.25
100	7.25	9.35	11.45
125	7.85	10.55	12.65
150	8.35	11.35	14.15
175	8.95	12.45	15.35
200	9.15	13.35	16.15
225	9.35	13.85	18
250	9.85	14.35	19.35



Figure 4. Graphical representation of execution time

Figure 4 given above shows the average execution time involved in secure data communication between cloud users in cloud computing network. As shown in the above graphical chart, the execution time is found to be directly proportional to the number of cloud user data. The above chart indicates that the execution time of different methods BVDNP-CS, CGST-FCM[1], HBRSS [2] are

denoted by three distinct colors namely green, blue and red respectively. However, the chart portrays that the execution time is found to be comparatively lesser using the BVDNP-CS method than the other two existing methods. The reason behind the improvement is that the deep learning-based Multi-linear Bernstein-Vazirani Signcryption and Unsigncryption efficiently performs the key generation, signcryption and unsigncryption. If the cloud user requires to obtain data from cloud service provider via trusted party, the cloud user initially checks the authenticity by comparing target value to that produced by perceptron. The cloud service provider validates the digital signature. Upon successful validation only, then the cloud service provider permits access to cloud users and sends requested data. This process takes minimum time than the existing methods.

Performance evaluation of storage overhead

Storage overhead refers to the amount of memory consumed by the Bernstein-Vazirani Key Generation algorithm for key generation process to achieve secure data communication in cloud computing network. The storage overhead is mathematically stated as given below.

$$SO = \sum_{i=1}^n DP_i * Mem[PPK(U_i) + PK(U_i) + PubK(U_i)] \quad (14)$$

From the above equation (14), storage overhead ' SO ' is measured on the basis of the cloud data or data packet to be sent between cloud users, and the memory consumed during the generation of three keys, partial private key ' $PPK(U_i)$ ', private key ' $PK(U_i)$ ' and public key ' $PubK(U_i)$ ' respectively. Table 3 noticed that the storage overhead of three distinct methods, BVDNP-CS, CGST-FCM [1] and HBRSS [2] according to the number of data packets. For experimental purpose, the numbers of cloud user data are taken in the ranges from 25 to 250. The overhead of the three methods are found to be increasing while increasing number of cloud user data. This is owing to the reason that the trusted party on behalf of the cloud service provider generates the three keys, i.e., partial private key, private key and public key keys for numerous cloud user data hence the memory consumed in key generation gets also increased. This is proved by the statistical analysis. Let us consider 25 cloud user data for performing simulation. The memory consumption of generating the private and public key pair using BVDNP-CS method is 150KB. Similarly, the memory consumption of CGST-FCM [1] and HBRSS [2] is observed as 250KB and 375KB while considering similar counts of cloud user data being used. In a similar manner, the storage overhead of distinct results is inferred for each method. The obtained results of the BVDNP-CS method are compared with the existing methods. The average of comparison results confirms that the BVDNP-CS method reduces the storage overhead by 20% when compared to CGST-FCM [1] and 39% when compared to the HBRSS [2].

Table 3
Tabulation for overhead using BVDNP-CS, CGST-FCM [1] and HBRSS [2]

Number of cloud user data	Overhead (KB)		
	BVDNP-CS	CGST-FCM	HBRSS
25	150	250	375
50	185	275	400
75	215	310	410
100	285	335	435
125	305	350	455
150	325	375	480
175	340	390	510
200	365	435	535
225	390	455	585
250	425	480	625

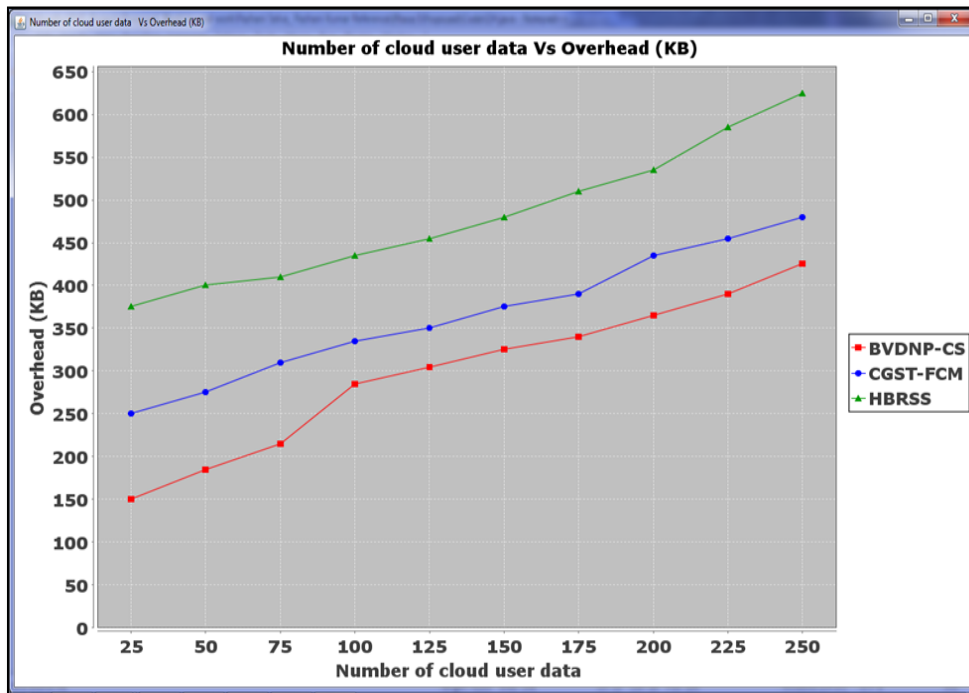


Figure 5. Graphical representation of overhead

Figure 5 shown above demonstrates the average storage overhead via different algorithms involved in the key generation. The horizontal axis denotes the number of cloud user data obtain in the ranges between 25 and 250. On the other hand, vertical axis denotes the storage overhead measured in terms of kilobytes (KB). Figure 5 inferred that the overhead of the BVDNP-CS method is found to be minimized than the existing methods. The Bernstein-Vazirani Key Generation algorithm is applied in the BVDNP-CS method for secure data access between cloud users in cloud computing network. The objective behind the

utilization of Bernstein–Vaziranifunction remains in addressing the problem quantumly or cracking keys quantumly with the aid of only single query on comparison to the existing methods that would require all ' n ' queries. This in turn would reduce the overhead.

Performance evaluation of data confidentiality rate

Finally, data confidentiality rate is measured on the basis of the cloud data as retrieved by the authorized cloud users to the total number of cloud users' data. The formula for measuring the data confidentiality rate is given below.

$$DCR = (U_D[Auth])/U_D * 100 \quad (15)$$

From the above equation (15), the data confidentiality rate ' DCR ' is measured on the basis of number of cloud user data accessed by authorized user ' $U_D[Auth]$ ' and the number of cloud user data ' U_D '. It is measured in terms of percentage (%). Finally, table 3 given below illustrates the experimental results of data confidentiality rate for 250 different cloud user data. A comparison of the BVDNP-CS method is made with the two existing methods, namely, CGST-FCM [1] and HBRSS[2] respectively. The results confirm that the BVDNP-CS method achieves better performance in terms of good data confidentiality rate than the traditional methods. This is inferred via numerical analysis. Let us consider 25 data for calculating the data confidentiality rate. By applying the BVDNP-CS method, 22 cloud user data were precisely accessed by the authorized cloud users and hence the data confidentiality rate was found to be 88%. On the other hand, by employing CGST-FCM [1] and HBRSS[2], 20 and 19 cloud user data were correctly accessed by authorized users. Therefore, the data confidentiality rates were observed to be 80% and 76%. Totally ten different simulations were performed for each method. The obtained results prove that the average data confidentiality of the BVDNP-CS method is higher by 14% and 23% when compared to the existing methods.

Table 4
Tabulation for data confidentiality rate using BVDNP-CS, CGST-FCM [1] and HBRSS [2]

Number of cloud user data	Data confidentiality rate (%)		
	BVDNP-CS	CGST-FCM	HBRSS
25	88	80	76
50	87.35	79.55	75.35
75	87	79.25	74.15
100	86.85	77.15	73.85
125	86.15	75.35	72.15
150	85.25	74.15	70.35
175	85	72.25	68.45
200	84.15	72	65

225	83.75	71.15	63.15
250	82	70	61

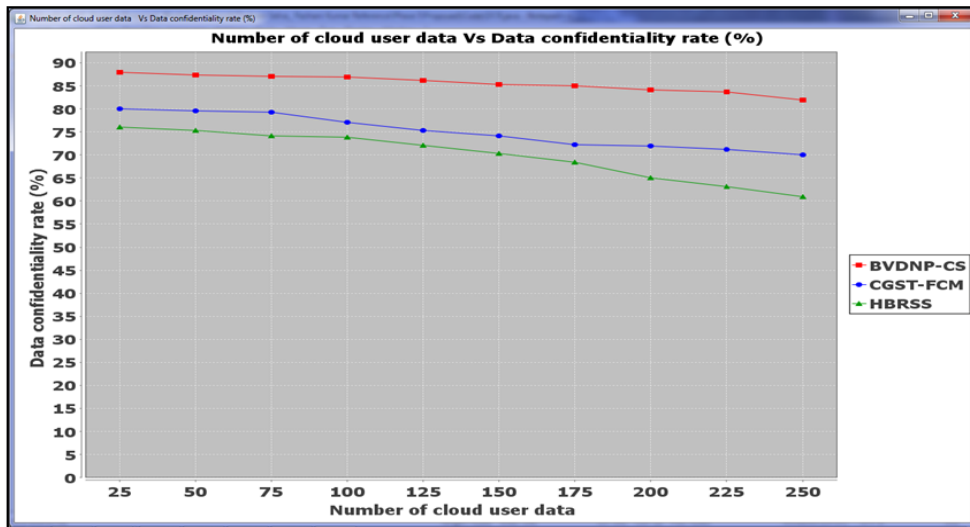


Figure 6. Graphical representation of data confidentiality rate

Figure 6 given above shows the data confidentiality rate using three distinct certificateless signcryption methods. The confidentiality rate in the proposed BVDNP-CS method is increased upon comparison with the other two existing methods [1, 2]. The reason behind this is due to the application of Multi-linear Bernstein–Vazirani Signcryption and Unsigncryption algorithm. By applying this algorithm, only upon successful matching between the entered cloud user row identifier and the cloud server database, the entered cloud user is authorized and followed by which granted with access and hence referred to as authorized user. Due to this, the cloud service provider via third party permits access to authorized cloud user and conducts both encryption and signature generation process. As a result, secure data communication in cloud computing network is ensured with good data confidentiality.

Conclusion

A novel data communication method BVDNP-CS is offered to provide the security using certificateless signcryption in cloud computing. The proposed BVDNP-CS method uses Bernstein–Vazirani Key Generation and Multi-linear Bernstein–Vazirani based signcryption to achieve high data confidentiality. The cloud service provider via trusted party permits access to the cloud users only after verifying and validating the authenticity with the Bernstein–Vazirani function. Then the Multi-linear Bernstein–Vazirani Signcryption is applied in the BVDNP-CS method for enhancing the security level by transmitting data packets in the form of ciphertext to the intended cloud receiver. Finally, the signature is verified and validated at the receiving end to decrypt the cloud user data. Experimental evaluation is carried out for analyzing the performance of BVDNP-CS method and traditional certificateless signcryption with distinct set of metrics. Comparisons were performed and the observed result infers that the proposed BVDNP-

CSmethod is performed well and is more effective than the earlier ones, having a higher data confidentiality rate, and lesser execution time as well overhead.

References

1. Chandrashekhar Meshram, Agbotiname Lucky Imoize, Sajjad Shaukat Jamal, Adel R. Alharbi, Sarita Gajbhiye Meshram, Iqtadar Hussain, "CGST: Provably Secure Lightweight Certificateless Group Signcryption Technique Based on Fractional Chaotic Maps", *IEEE Access*, Apr 2022
2. Hui Xie, Zhengyuan Zhang, Qi Zhang, Shengjun Wei, Changzhen Hu, "HBRSS: Providing high-secure data communication and manipulation in insecure cloud environments", *Computer Communications*, Elsevier, Apr 2021
3. Fursan Thabit, Sharaf Alhomdy, Sudhir Jagtap, "A new data security algorithm for the cloud computing based on genetic techniques and logical-mathematical functions", *International Journal of Intelligent Networks*, Elsevier, Mar 2021
4. Dilip Venkata Kumar Vengala, D. Kavitha, A. P. Siva Kumar, "Secure data transmission on a distributed cloud server with the help of HMCA and data encryption using optimized CP-ABE-ECC", *Cluster Computing*, Springer, Apr 2020
5. Amr M. Sauber, Passent M. El-Kafrawy, Amr F. Shawish, Mohamed A. Amin, Ismail M. Hagag, "A New Secure Model for Data Protection over Cloud Computing", *Computational Intelligence and Neuroscience*, Hindawi, Nov 2021
6. Jun Ma, Minshen Wang, Jinbo Xiong, Yongjin Hu, "CP-ABE-Based Secure and Verifiable Data Deletion in Cloud", *Security and Communication Networks*, Wiley, Mar 2021
7. Rongbin Xu, Jianguo Wu, Yongliang Cheng, Zhiqiang Liu, Yuanmo Lin, Ying Xie, "Dynamic Security Exchange Scheduling Model for Business Workflow Based on Queuing Theory in Cloud Computing", *Security and Communication Networks*, Wiley, Aug 2020
8. Hua Yi Lin, Meng-Yen Hsieh, "A dynamic key management and secure data transfer based on m-tree structure with multi-level security framework for Internet of vehicles", *Connection Science*, Taylor & Francis, Mar 2022
9. Xi Luo, Lihua Yin, Chao Li, Chonghua Wang, Fuyang Fang, Chunsheng Zhu, Zhihong Tian, "A Lightweight Privacy-Preserving Communication Protocol for Heterogeneous IoT Environment", *IEEE Access*, Apr 2020
10. Tejaswini Apte, Priti Kulkarni, "Network Communication Encoding: A Study for Authentication Protocols", *Computer Science*, Springer, Feb 2022
11. M. G. Aruna, Mohammad Kamrul Hasan, Shayla Islam, K. G. Mohan, Preeta Sharan, Rosilah Hassan, "Cloud to cloud data migration using self sovereign identity for 5G and beyond", *Cluster Computing*, Springer, Oct 2021
12. Yang Changsong, Tao Xiaoling, Zhao Feng, Wang Yong, "Secure Data Transfer and Deletion from Counting Bloom Filter in Cloud Computing", *Chinese Journal of Electronics*, Mar 2020
13. Abdul Rehman, LIU Jian, Muhammad Qasim Yasin, LI Keqiu, "Securing Cloud Storage by Remote Data Integrity Check with Secured Key Generation", *Chinese Journal of Electronics*, May 2021

14. Deepnarayan Tiwari, G. R. Gangadharan, "SecCloudSharing: Secure data sharing in public cloud using ciphertext-policy attribute-based proxy re-encryption with revocation", Wiley, Nov 2017
15. Pan Yang, Naixue Xiong, Jingli Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey", IEEE Access, Jul 2020
16. Hesham A. El Zouka, "An Efficient and Secure Vehicular Networks Based on IoT and Cloud Computing", Computer Science, Springer, Apr 2022
17. Manoj Kumar, Harsh Kumar Verma, Geeta Sikka, "A secure data transmission protocol for cloud-assisted edge-Internet of Things environment", Wiley, Jan 2020
18. Qin Liu, Guojun Wang, Xuhui Liu, Tao Peng, Jie Wu, "Achieving reliable and secure services in cloud computing environments", Computers and Electrical Engineering, Elsevier, Aug 2016
19. Pan Jun Sun, "Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions", IEEE Access, Oct 2019
20. Mehedi Masud, Gurjot Singh Gaba, Karanjeet Choudhary, Roobaea Alroobaea, "A robust and lightweight secure access scheme for cloud based E-healthcare services", Peer-to-Peer Networking and Applications, Springer, May 2021
21. Suryasa, I. W., Rodríguez-Gámez, M., & Koldoris, T. (2021). Health and treatment of diabetes mellitus. *International Journal of Health Sciences*, 5(1), i-v. <https://doi.org/10.53730/ijhs.v5n1.2864>
22. Rahmadeni, A. S. ., Hayat, N. ., Alba, A. D. ., Badri, I. A. ., & Fadhila, F. . (2020). The relationship of family social support with depression levels of elderly in 2019 . *International Journal of Health & Medical Sciences*, 3(1), 111-116. <https://doi.org/10.31295/ijhms.v3n1.188>